Glossary

Access Control Entry (ACE) — A single entry in an access control list that grants or denies permission to an NTFS or Active Directory object.

Access Control List (ACL) — A series of access control entries that define the level of access security that principals have to an NTFS or Active Directory object.

access token — Created for a user when the user logs on to a Windows 2000 computer or a Windows 2000 network. The access token includes the user's SID, the SIDs of all the groups to which the user belongs, and the user's rights and privileges.

Active Directory — The directory service in Windows 2000.

Active Directory integrated zone — A DNS zone that is stored within the active directory.

Active Directory schema — A list of object classes and attribute classes available in Active Directory.

Active Directory Tree — A grouping of one or more Windows 2000 domains.

Application server mode — A mode within Terminal Services that allows clients to run a common server-based application.

auditing — The option in Windows 2000 for monitoring administrative actions, logons and object access.

Authentication Header Protocol (AH) — A part of IPSec that provides data authentication, integrity, and anti-replay protection for the data transmitted over the connection.

Authentication Service — The service in Windows 2000 that gives users access to the network.

back-to-back DMZ — Two firewalls used to create a protected network segment between the internal network and the Internet.

Bandwidth Allocation Protocol (BAP) — A protocol used to dynamically manage multiple links for remote access.

callback — The option available on a remote access connection in which you can configure the remote access server to call a user at a specified phone number after the client has connected and has been authenticated.

caller ID — The option available on a remote access connection in which you can configure the dial-up connection so that a user can dial in from only one specific phone number.

Certificate Authority (CA) — A certificate server that assigns certificates to other certificate servers or clients.

certificate revocation lists (CRLs) — Lists maintained by CAs of certificates that have been revoked. Clients and servers should check the CRL before granting access based on a certificate.

Certificate Server — Microsoft's standards-based PKI service available for Windows 2000.

Certification Authority (CA) — A server that is used to grant and manage user and computer certificates in a Public Key Infrastructure.

child domain — A domain that is connected to another parent domain in an Active Directory tree. The child domain shares a contiguous DNS namespace with the parent domain.

client authentication — Used to insure the authenticity of the client by checking the validity and authenticity of the client's certificate.

Computer Local group — A group that resides in the local directory database of a workstation or standalone server.

delegation — The process of distributing and decentralizing the administration of Active Directory.

demand-dial router — A router that initiates a dial-up connection to a remote location only when needed.

Demilitarized Zone (DMZ) (screened subnet) — A protected area between the internal network and the Internet, separated by firewalls. Internet-accessible resources are placed within this protected area to keep a distinct separation from the internal network.

denial-of-service (DoS) attack — Any type of attack on a network service that results in legitimate users of that service not being able to access the service.

digital certificates — A digital entity assigned to a user or computer that is used to vouch for the identity of the certificate holder.

digital signature — A mechanism used to insure the identity of the sender of a message and also to insure the integrity of the message.

directory service — A central database that stores information about network-based objects such as computers, printers, users, and groups.

Discretionary Access Control List (DACL) — Lists the security principals that have been assigned permission to the object, as well as the level of permissions for each security principal.

Distribution group — A group that is used to organize users for specific tasks like sending batch e-mail messages.

DNS zone — Represents a part of the DNS namespace that contains resource records for that zone's DNS domains.

DNSUpdateProxy security group — Objects created in DNS by any member of this group have no security, enabling any authenticated user to take over ownership of the resource record.

domain — A collection of objects that share the same user account database and security policy.

domain local group — A group of common objects created on a domain controller and used to control permissions for resource access.

Domain Name System (DNS) — A hierarchical and searchable database of computer (host) names and IP addresses. Windows 2000 also incorporates SRV records into the database to locate network services.

Dynamic DNS — A mode of Windows 2000 DNS that allows clients to automatically enter and modify their own resource records.

Dynamic Host Configuration Protocol (DHCP) — A protocol that is used to assign IP addresses and other various options to network clients.

Encapsulating Security Payload (ESP) — A second protocol used in IPSec that provides data authentication, integrity, and anti-replay protection, as well as encrypts the data transmitted over the connection.

Encrypted File System (EFS) — The option available in Windows 2000 that enables a user to encrypt specified files on the computer hard disk. The encrypted files can be recovered only by the user and the designated recovery agent.

encryption — The process of scrambling data as it is transmitted between two points to ensure confidentiality.

enterprise CA — An implementation of Windows 2000 Certificate Server that requires Active Directory and is completely integrated with Active Directory. This integration can simplify the administration of certificates, because you can configure policies that automate the process of granting, renewing, and revoking certificates.

Extensible Authentication Protocol (EAP) — An authentication protocol available in Windows 2000. EAP is different from the other options in that it is really a standard for designing other authentication processes, such as certificate-based authentication.

firewall — A device that is located between a corporation's internal network and the Internet. It is designed to allow internal users to access the Internet while restricting or blocking access from the Internet to the internal network. A firewall may be a dedicated hardware device or an application that runs on a computer.

firewall — A software-based or hardware-based component that allows only specific types of traffic in or out of the internal network.

firewall rule — The combination of multiple packet filters configured on a firewall.

forest — A collection of Active Directory Trees connected by trust relationships. The trees in a forest do not share a contiguous namespace.

Generic Routing Encapsulation (GRE) — The protocol used by PPTP to encapsulate the encrypted packets that are being transmitted across the Internet.

global catalog — A subset and collection of attributes from every object within the forest.

Global group — A security group used to create collections of users or computers.

Group Policy — An object created that allows centralized management of user and computer configuration settings.

hierarchical CA structure — A configuration of certificate authorities into a hierarchical structure where each CA issues the certificate for the CA underneath it in the hierarchy. All CAs in the same hierarchy share the same root CA.

Internet Authentication Service (IAS) — Microsoft's implementation of the Remote Authentication Dial-in User Service (RADIUS).

Internet Connection Sharing (ICS) — An option that can be configured on a remote access connection that makes it possible for multiple users in a small office to share a single connection to the Internet or another network.

Internet Explorer Administration Kit (IEAK) — Can be used to design customized Web browser implementations that enforce and lock security and proxy configuration settings.

Internet Explorer Content Advisor — Can be used to control the types of Web content that users can access.

Internet Key Exchange (IKE) — An IPSec component that manages Security Associations and manages the generation and exchange of the keys between the two systems.

Internet Protocol Security (IPSec) — A protocol used for data authentication and encryption over a TCP/IP network. Also referred to as IP Security.

IPSec driver — Receives the filter list from the IPSec Policy configured on the machine. The IPSec driver also is in charge of the IKE to make sure that the key exchange process is taking place between the two machines.

Kerberos version 5 — The default authentication protocol used when Windows 2000 clients log on to a Windows 2000 domain.

Key Distribution Center (KDC) — The authenticating server in a Kerberos authentication model. In a Windows 2000 domain, the Domain Controllers are KDCs.

Layer 2 Tunneling Protocol (L2TP) — A protocol that provides authentication services over public networks. Often used in conjunction with IPSec to create secure VPN connections.

Layer Two Tunneling Protocol (L2TP) — One of the virtual private network protocols supported by Windows 2000.

message digest — The result of a mathematical hash being applied to a message. The message digest is used as part of a digital signature to insure that the message was not tampered with while it was transmitted on the network.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) — One of the authentication protocols available with Windows 2000 remote access. It is based on a challenge and response handshake for authentication. MS-CHAP is quite secure because the password is never sent on the network in an unencrypted form.

Microsoft Point-to-Point Encryption (MPPE) — The encryption algorithm used by PPTP to encrypt the packets before they are transmitted on the network. The keys used for the encryption are based on the user's name and password.

MS-CHAP version 2 — Similar to MS-CHAP, but with enhanced security options.

mutual authentication — The process of two points (routers) authenticating to each other to ensure that packets are sent only to authorized routers.

Network Access Server (NAS) — The remote access server that clients connect to in a RADIUS implementation. The NAS acts as the RADIUS client in the authentication process by forwarding all authentication requests to the RADIUS Server.

Network Address Translation (NAT) — Protects a network by replacing the source internal address and ports of all outgoing packets with a single public IP address.

NTFS permissions — Used to control the level of access security that principals have to folders and files on an NTFS partition. NTFS permissions are applied both when a user logs on locally to a computer and when the user accesses the information through a network share.

NTLM authentification (Windows NT Lan Manager) — The authentication protocol used by down-level clients such as Windows NT when authenticating a user on a Windows 2000 network.

Open Shortest Path First (OSPF) — A link-state routing protocol where each router builds a routing table that includes the entire local network, as well as links to external networks.

organizational unit (OU) — A grouping of common objects, such as users and groups, that all share the same departmental and security policies.

packet filter — Describes various characteristics of a network packet that define whether the packet will be allowed or denied access through a firewall.

packet filtering — Consists of setting rules and conditions on how packets are sent and received on a network.

packet sniffer — A tool that can be used to capture all of the packets that are sent on a network. The packets can then be analyzed for data or passwords.

Point-to-Point Tunneling Protocol (PPTP) — Network technology that gives clients using TCP/IP, IPX, or NetBEUI the ability to create a secure VPN over a public TCP/IP network, such as the Internet.

prestaged clients — A computer account that is precreated in Active Directory before the operating system is installed on the computer.

Pretty Good Privacy (PGP) — A service that encrypts and signs e-mail between two users using the same third-party software.

private key — A key that is part of a certificate and is known only to the user who holds the certificate. It can be stored on the computer's hard drive, or as part of a roaming profile, or on a different device, such as a smart card.

proxy server — A service that can restrict Internet access by user name or group membership, protocol, or by Web site address.

public key — A key that is made available to anyone who asks for it. The public key is attached to the certificate.

public key infrastructure (PKI) — A security model that uses certificates and private and public keys to authenticate users and computers and to encrypt and digitally sign data.

Public Key Infrastructure (PKI) — A system of protecting data that is sent across a public network such as the Internet by authenticating and validating users and by encrypting traffic on the network. The components that make up a PKI include certificate authorities, certificates, and public and private keys.

recovery agent — A user that has been assigned a recovery certificate so that the user can decrypt any file that has been encrypted by users. By default, the administrator on a standalone computer and the administrator of the first Domain Controller in a domain are the only recovery agents.

remote access policies — Policies that can be configured on a Windows 2000 RRAS server that enable enhanced options for managing remote access user connections.

remote access service (RAS) — A service that is used to give remote access clients access to a network by using either a dial-up or VPN connection.

Remote administration mode — One of the modes available in Windows 2000 terminal servers that is used to provide administrators with remote administration capabilities to Windows 2000 servers.

Remote Authentication Dial-in User Service (RADIUS) — An open standard that is widely used for remote access authentication in large, distributed environments such as ISPs. The purpose of RADIUS is to centralize the management of remote access users and policies in an environment in which the remote access servers might be widely distributed.

Remote Desktop Protocol (RDP) — The protocol used in Windows 2000 Terminal Services. Only screen write and keystroke information is sent using RDP.

Remote Installation Services (RIS) — A service available in Windows 2000 that can be used to simplify the deployment of Windows 2000 Professional to desktop computers.

Request for Comment (RFC) 1918 — States that certain IP Addressing ranges have been designated as private. The private IP address ranges include 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255.

reverse proxy (static) mappings — Configuration settings that direct incoming traffic to a particular resource protected behind the firewall.

root CA — The top server in a CA hierarchy. The root CA issues its own root certificate.

root domain — The first domain installed in an Active Directory structure.

router — A networking device, either software-based or hardware-based, that controls and forwards packets between networks.

Routing and Remote Access Service (RRAS) — The Windows 2000 component that provides the remote access service, as well as routing functionality.

Routing Information Protocol (RIP) — A distance vector routing protocol that can be used to automatically build the routing table in Windows 2000. A distance vector protocol means that the routing table consists of routes that are configured with a distance (hop count) and a vector (the gateway to the destination network).

routing protocols — Protocols used to automatically update the routing table entries.

routing table — A list of all the networks that a router has identified, and the addresses that the router can use to forward messages to that network.

secedit.exe — A command–line tool used to analyze and configure security templates.

secure dynamic updates — A mode of Windows 2000 DNS that allows Access Control lists to be edited on DNS zones or resource records. This mode also allows only the hosts that own a record to be able to modify the record.

Secure Sockets Layer (SSL) and **Transport Layer Security (TLS)** — Two open standards that require PKI to authenticate and encrypt data flowing between Web servers and Web clients.

Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3 — A proposed standard for secure e-mail where e-mail can be encrypted and digitally signed as it is sent between two users.

Security and Configuration tool set — A set of tools that help create, analyze, and apply security template configurations.

Security Association (SA) — Defines the authentication and encryption process for the IPSec communication.

Security group — A group of security principals collected for the purpose of applying specific permissions to resources.

Security Identifier (SID) — A unique number identifying all security principals on a Windows 2000 network. Windows 2000 uses SIDs when managing permissions, rather than user or group account names.

Security Policy Template — A file that contains a collection of security settings that can be applied to users or computers by using the Security Configuration Tool set.

security principal — Any object in Windows 2000 that can be used to assign permissions to other objects. Only users, groups, computers, and network services can be security principals.

security zones — One of four classifications used in Internet Explorer to assign security levels to web sites. The four classifications are the Local Intranet zone, Internet zone, Trusted Sites zone, and the Restricted Sites zone.

server authentication — The process of ensuring that a server is authentic and not an imposter. The authentication in this case is certificate-based; if the server can prove that it has a valid certificate that the client trusts, then the client assumes that the server is authentic.

Server Message Block (SMB) — (Also known as Common Internet File System) A protocol used between computers to share resources such as files, printers, and communication connections, including named pipes and mail slots.

Service Record (SRV Record) — A DNS resource record that reveals the name and IP address for special Windows 2000 services, such as the global catalog or site information.

session key (also called **bulk encryption key** or **symmetric key)** — The key that is used to encrypt a message when it is sent across the network. Both the sending and receiving computers use the same session key, which is encrypted and decrypted using the private and public keys.

session ticket — A ticket used in a Kerberos authentication model to gain access to computers and resources on a network.

share permissions — Permissions used to manage user access to shares on a Windows 2000 server. Share permissions are effective only when the user accesses the shares across a network connection, not when the user logs on the computer locally.

Simple Mail Transfer Protocol (SMTP) — The protocol used to send all Internet mail. The primary security concern with SMTP is that all e-mail sent with SMTP is sent in clear text.

Simple Network Management Protocol (SNMP) — Used to assist the administrator in managing and configuring network resources.

SMB signing — Refers to the option to digitally sign each message block that is sent to or from a server and client. This digital signature authenticates both computers in the network communication and provides data integrity.

SNMP agent — A service that runs on a device that reports status messages to an SNMP management station.

SNMP community — A collection of SNMP agents that are all managed together as a group and that all have a common community name.

SNMP management station — The central administrative point that allows the administrator to query, monitor, and receive status messages from any SNMP agent configured on the system.

SNMP trap — An alert message sent to a configured management station.

social engineering — A method used by people attacking the network. The attacker convinces legitimate users on the network to provide the attacker with confidential information such as logon names and passwords.

social engineering attack — An attack aimed at the users of a technology rather than at the technology itself. The most common way to launch a social engineering attack is to contact the user and present false credentials.

SSL handshake — The process of authenticating servers and clients, and creating a session key that can be used by SSL to encrypt all data.

standalone CA — An implementation of Windows 2000 Certificate Server that does not require Active Directory and can be integrated with third-party CAs.

standard primary zone — A DNS zone that stores its read/write database within a text file on the hard drive.

standard secondary zone — A copy of the primary DNS zone that is read-only.

static routes — Entries that have been manually entered into the routing table to assist the router in forwarding packets to networks not directly connected to the router.

subordinate CA — A CA that is at a lower level in the CA hierarchy. Subordinate CA certificates are always issued by the CA immediately above the subordinate CA in the CA hierarchy.

System Access Control List (SACL) — Lists the security principals whose access to a resource needs to be audited.

Terminal Services — A service in Windows 2000 where clients can run applications entirely on a terminal server.

three-homed firewall DMZ — A DMZ configuration where a single firewall is set up with one network adapter connected to the Internet, a second adapter connected to the private network, and a third adapter connected to the DMZ.

Ticket Granting Ticket (TGT) — A ticket granted to a user when the user logs on to a Windows 2000 domain. The TGT is used to acquire session tickets.

transitive trust — The link between domains in Active Directory.

Transport mode — An IPSec mode implemented when communications need to be encrypted from an originating computer through to a target computer.

trust path — A mechanism for computers with certificates from different CAs to trust each other's certificates. If the two computer certificates have the same root CA, then they share a trust path and will trust each other's certificates.

Tunnel mode — An IPSec mode where the transmitted data is protected only between two points in a communication channel, thus forming a protected "tunnel" for part of the channel.

Universal group — A collection of objects that can be assigned permissions throughout the entire Active Directory Forest.

Virtual Private Network (VPN) — Used to encapsulate and encrypt packets to provide security between two remote networks over a public network.

wide area network (WAN) — A computer system that connects two or more remote locations over a wide geographical area.

X.509 Version 3 — The current standard for PKI certificates. The certificate includes information about the person, computer, or service to which the certificate has been issued, information about the certificate itself, and information about the Certificate Authority that issued the certificate.

zone transfer — The transfer of changes from a standard primary DNS zone file to a standard secondary zone.